UOT 004.9:351

İmamverdiyev Y.N.[1], Qarayeva G.B[1,2]
[1]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[2]Azərbaycan Dövlət Pedaqoji Universitetinin Şəki filialı, Şəki, Azərbaycan
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru

BOTNETLƏR VƏ ONLARIN AŞKARLANMASI ÜSULLARI

Botnetlər kiber-hücum infrastrukturunda mühüm yer tuturlar. Botnet yoluxmuş kompüterlərdən və onları idarə edən botmasterlərin istifadə etdikləri C&C serverlərdən ibarət şəbəkədir. Bəzən bu şəbəkəyə milyonlarla kompüter cəlb edilir. Botnetlər daim inkişaf edir, onların strukturu, istifadə etdikləri protokollar, yoluxdurma üsulları, hücum məqsədləri daim dəyişir. Məqalədə botnetlərin arxitekturası, təsnifatı və aşkarlanma üsulları araşdırılmışdır.

Açar sözlər: *botnet, C&C server, honeypot, DDoS hücum, botnetlərin aşkarlanması üsulları.*

Giriş

Botnet – "robot" və "network" sözlərinin birləşməsindən yaranmışdır, xüsusi bot proqramlarla yoluxmuş kompüterlərin şəbəkəsini bildirir. Bot istifadəçi kompüterində gizli quraşdırılan və bədniyyətliyə yoluxmuş kompüterin resurslarından istifadəçinin xəbəri olmadan istifadə etməklə, müəyyən əməlləri yerinə yetirməyə imkan verən zərərli proqramdır. Botnet şəbəkələrini çox vaxt verilmiş əmrləri avtomatik yerinə yetirən zombi-kompüter şəbəkələri də adlandırırlar.

Botnetlər bir çox onlayn kiber-cinayətdə, böyük miqyaslı DDoS hücumlarda (*ing. Distributed denial-of-service – paylanmış xidmətdən imtina hücumu*), spam göndərilməsində, "klik" saxtakarlığında, məxfi informasiyanın oğurlanmasında və s. zərərli fəaliyyətlərdə istifadə olunurlar. Botnetlər tərəfindən yoluxdurulmuş kompüterlərin sayı və coğrafi paylanması botmasterlərin asan əldə edilə bilən proqram kodlarından və geniş dəstəkləyici əlaqələrdən istifadə etməsindən asılıdır. Belə şəbəkələrdən əsasən qazanc məqsədilə istifadə olunur. Belə ki, botmasterlər istənilən vaxt botnetləri icarəyə verib, onlayn hücumlar həyata keçirə bilirlər. Bu da kibercinayətkarların aşkarlanmasını kifayət qədər çətinləşdirir. Milyonlarla kompüterin cəlb edildiyi botnetlər məlumdur və hər gün yeniləri yaranmaqda davam edir.

Son onillik ərzində botnetlərin aşkarlanması üçün üsulların işlənməsi sahəsində müəyyən elmi nailiyyətlər əldə edilmişdir. Botnetlərə müxtəlif aspektlərdən yanaşılmış və müxtəlif texniki prinsiplərə əsaslanan bir çox aşkarlama üsulları işlənmişdir. Bu yanaşmalar içərisində ən çox diqqəti cəlb edən və kifayət qədər əhəmiyyətli nəticələr əldə etməyə imkan verən üsullar maşın təlimi (*ing. Machine Learning*) (MT) üsullarına əsaslanan aşkarlamadır.

İnternetin xidmətlərinin artması və həyatımızdakı əvəzedilməz rolu istifadəçi verilənlərinin təhlükəsizliyi, məxfilik, tamlıq kimi bir sıra problemlərin də yaranmasına səbəb olmuşdur. Son 20 il ərzində İnternet və İnternet-əsaslı tətbiqlər həyatımızın tamamlayıcı hissəsinə çevrilmişdir. Təhsil, səhiyyə, bank işi, ictimai və sosial həyat və s. sahələrin İnternet üzərindən fəaliyyəti də təhlükəsizlik problemlərinin həllini çətinləşdirir. İnternetdə təhlükəsizlik təhdidlərinin əsasını zərərli proqram təminatı (*ing. malware*) təşkil edir. Zərərli proqramla yoluxmuş kompüterdə istifadəçi verilənləri təhlükə altına düşür. Zərərli proqramlarla mübarizə üsullarına paralel olaraq belə proqram təminatının yayılma və yoluxdurma mexanizmləri, zərərli fəaliyyətlərin növləri də dəyişmiş və inkişaf etmişdir.

Zərərli bot proqramları (*ing. bot malware*) [1, 2] kompüter proqramlarını digər zərərli proqramlar – viruslar, troyanlar, rootkitlər, soxulcanlar və s. kimi asanlıqla yoluxdururlar. Lakin bot proqramlarının əsas fərqi və üstünlüyü C&C əlaqə kanalından istifadə edərək bədniyyətli ilə əlaqə saxlaya bilməsidir. Bu kanal vasitəsilə botmaster bot proqramı uzaqdan idarə edir və öz istəklərini daha rahat həyata keçirir.

Botmasterlər böyük miqyasda zərərli və qeyri-qanuni fəaliyyət üçün yüksək səviyyədə paylanmış və öz aralarında əməkdaşlıq edə bilən bot platformaları yaradırlar. Botnetlər fərdi kompüterləri, korporativ və təhsil şəbəkələrini, avtomatik idarəetmə sistemlərini və s. əhatə edə

bilərlər. Botnetlərin gücü yalnız onların sayı ilə deyil, zərərli fəaliyyətləri ilə də ölçülür. Belə şəbəkələr spam göndərir, DDoS hücumlar həyata keçirir, "klikləmə" saxtakarlığı edir, zərərli proqramları, qeyri-qanuni kontentləri və reklamları yayır, məxfi məlumatları toplayır, kritik infrastrukturlara hücumlar edə bilirlər [3].

Botnetlərin neytrallaşdırılması mövcud botnetlərin aşkarlanması və müvafiq müdafiə tədbirlərinin həyata keçirilməsindən ibarətdir. Botnetlərin aşkarlanmasına müxtəlif yanaşmalar mövcuddur ki, bunlar da əsasən botnetlər tərəfindən yaradılan şəbəkə trafikinin müşahidəsi və bot davranışlarının analizinə əsaslanır. Bu sahədə ən çox istifadə olunan üsullar qurulmuş obrazlara əsasən zərərli trafiki aşkarlamağa imkan verən MT metodlarıdır. MT əsasında aşkarlamada əsas yanaşma seçilmiş şəbəkə trafikindən botnetlərə uyğun obrazların yaradılması və onların effektiv aşkarlanmasını təmin etməkdir.

Botnetlərlə mübarizə iki mərhələdə aparıla bilər. Birincisi, botla yoluxmadan qorunmaq (bu birbaşa istifadəçilərin üzərinə düşür), ikincisi isə, yoluxmuş qurğuların aşkarlanması və botnetin fəaliyyətinin dayandırılması. Botnetlərin istifadə etdiyi yoluxma üsullarının müxtəlifliyi, onların arxitekturasının kifayət qədər öyrənilməməsi, istifadəçilərin qorunma yollarından məlumatsızlığı botnetlərin yaranmasının əsas səbəblərindəndir.

Hazırda botnetlər və onların istifadə olunduğu sahələr sürətlə genişlənir. Botnetlərin qurulması və idarə edilməsi üsulları, həmçinin hücumların növləri artdıqca, yeni mübarizə üsullarının işlənməsi də aktual olaraq qalır.

Botnetlərin qısa xarakteristikası

Botnet zərərli proqramlarla yoluxmuş və bədniyyətli tərəfindən idarə edilə bilən kompüterlər şəbəkəsidir. Belə şəbəkədəki hər bir qurğu bot və botnetləri idarə edən bədniyyətlilər botmaster adlanır. Botmasterlər botnetləri müxtəlif məqsədlər üçün istifadə edirlər. Botmasterlər işə bot toplamaqla, yəni yeni kompüterlər ələ keçirməklə başlayırlar. Bunun üçün müxtəlif üsullardan istifadə olunur, məsələn, viruslar və ya digər zərərli proqramlar, e-poçt, spam, müxtəlif məqsədli cəlbedici şəkillər, reklam və s. Müasir bot cəlbetmə üsullarından ən çox istifadə olunanı çox sayda istifadəçisi olan sosial şəbəkələrin imkanlarından istifadə edilərək həyata keçirilən üsullardır (saxta hesablar, səhifələr, reklam və s. yaymaqla). Botmasterlər tərəfindən yayılan belə vasitələrin istifadəçi tərəfindən yüklənməsi nəticəsində həmin proqram kompüterdə qurulmuş olur. Kompüter botla bir dəfə yoluxduqda, o, botnet idarəetmə mərkəzinə bağlanır və əmr gözləyir. Yoluxmuş kompüterin açıq vəziyyətdə olması onun botmaster tərəfindən idarə edilməsi üçün kifayətdir. Belə istifadə istifadəçinin icazəsi olmadan yerinə yetirilir.

Botnetlər müxtəlif məqsədlər üçün istifadə olunurlar. Ən çox istifadə olunan məqsədlər aşağıdakılardır [4]:

1) Spam göndərilməsi. Bəzi mənbələrə görə [5], İnternet trafikinin 90%-dən çoxunu spam təşkil edir. Belə spamların 95%-dən çoxu botnetlər tərəfindən göndərilir. Spamın botnetlər tərəfindən yayılmasının botmasterlər üçün əsas üstünlükləri spamı qəbul edən tərəfin spamı göndərən tərəflə qanuni yollarla mübarizə apara bilməməsi və daha böyük həcmdə spamın yayıla bilməsidir;

2) DDoS hücumları. Botmasterlər botnetlərdən istifadə edərək veb-saytlara eyni anda böyük sayda müraciətləri təşkil edirlər. Belə olduqda, veb-serverdə gecikmə və ya tamamilə xidmətdən imtina vəziyyəti yaranır. Ən çox istifadə olunan DDoS hücumlarının bir növü də Syn-hücumlarıdır (*ing. Syn Flood*). Bundan əlavə, DoS hücumların digər bir növü olan Degradation of Service (Xidmətin tənəzzülü) hücumlarından da istifadə olunur;

3) İnformasiya oğurluğu. Belə məlumatlar bir çox sahələri əhatə edir: gizli saxlanılan məlumatlar (iqtisadi, elmi, tibbi və s.), dövlət əhəmiyyətli məlumatlar (hərbi sirlər, dövlət əhəmiyyətli sənədlər və s.), plastik kartlar haqqında məlumatlar, şəxsi məlumatlar (ünvan, telefon nömrəsi, istifadəçi adı/parol, PIN-kodlar və s.);

4) "Klikləmə" saxtakarlığı (*ing. Click fraud*). Veb-saytların, şəxsi bloqların, sosial şəbəkə səhifələrinin istifadəçi sayını süni olaraq artırmaq məqsədilə, həmçinin elektron səsvermə

sistemlərində klik sayı artırmaq (və ya azaltmaq) üçün botnetlərdən geniş istifadə olunur;

5) "Phishing" hücumları üçün infrastruktur yaratmaq;

6) Digər zərərli proqramları yaymaq, məsələn, casus proqramların, reklam materiallarının yayılması və s.

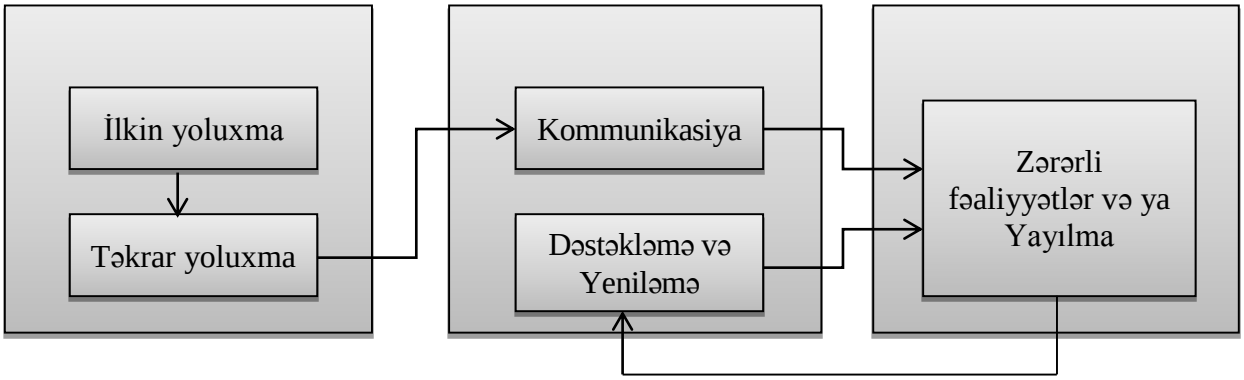
Botnet fenomeni

Botnetlər C&C əlaqə üsullarının müxtəlifliyi və zərərli fəaliyyətlərinin məqsədlərinə görə kompleks və hərtərəfli araşdırılması vacib olan fenomenlərdən biridir. Bundan əlavə, botmasterlər aşkarlanmanın çətinləşdirilməsi, bəzən də mümkün olmaması üçün botnetin işləmə üsullarını vaxtaşırı təkmilləşdirirlər. Botnet fenomenini daha yaxşı başa düşmək üçün botnetin fəaliyyət dövrü, C&C əlaqə kanalları, elastiklik və dayanıqlıq üçün istifadə etdikləri üsullar öyrənilməlidir.

Botnetin fəaliyyət dövrü

Botnetin fəaliyyət dövrü aşkarlama üsullarının seçilməsi üçün həlledici amillərdən biridir. Bir çox ədəbiyyatlarda botnetin fəaliyyət dövrü üç mərhələyə bölünmüşdür (şəkil 1) [6, 7]:

- yoluxma mərhələsi;
- kommunikasiya mərhələsi;
- hücum mərhələsi.



Şəkil 1. Botnetin fəaliyyət dövrü

Birinci mərhələdə kompüter hər hansı yolla xüsusi bot proqramla yoluxur. Yoluxma mərhələsi özü də iki altmərhələyə bölünür: ilkin və təkrar yoluxma. İlkin yoluxma zamanı kompüterə zərərli "yükləyici" yoluxdurulur. İlkin yükləmə müxtəlif yollarla: zərərli veb-saytlardan icazəsiz yükləmə zamanı, e-poçt mesajı əlavələri, yoluxmuş yaddaş qurğuları və s. vasitəsilə baş verə bilər. Uğurlu ilkin yükləmədən sonra təkrar yükləmə başlayır. Botnet zərərli proqramı müxtəlif protokollar: FTP, HTTP, HTTPS və ya hər hansı P2P protokol istifadə edərək kompüterə yüklənir və botmasterlə kommunikasiyanı gözləyir.

Kommunikasiya mərhələsində C&C server və botlar arasında təlimatların qəbul olunması, botmaster tərəfindən yenilənməsi, həmçinin botun statusunun yoxlanması üçün daim əlaqə yaradılır. Kommunikasiya bir neçə əməliyyatla həyata keçirilir: uğurlu yoluxdurmadan sonra C&C serverə qoşulma cəhdləri, yoluxmuş maşın təkrar işə düşdükdə yenidən qoşulma cəhdləri, yoluxmuş maşının statusunu yoxlamaq üçün vaxtaşırı əlaqə cəhdləri, C&C tərəfindən zərərli kodların yenilənməsi və ya əmrlərin digər botlara yayılmasının təmin edilməsi cəhdləri. Zombi kompüterlər və C&C server arasında kommunikasiya müxtəlif yollarla həyata keçirilir.

Hücum mərhələsində botlar botmasterin məqsədinə uyğun olaraq birbaşa zərərli fəaliyyətlərlə məşğul olurlar. DDoS hücumlar edir, e-poçt spamı kampaniyaları başladır, oğurlanmış informasiyanın yayılmasını həyata keçirir, onlayn fəaliyyət göstərən sistemlərin, sorğuların işini idarə edir və s. Bu mərhələdə botlar yayılma fəaliyyəti, yeni botların yoluxdurulması ilə də məşğul olurlar.

C&C əlaqə kanalı

Botnetlərin təsnifatı onların arxitekturasına və idarə edilməsi üçün istifadə edilən protokollara əsaslanır. Botnetləri xarakterizə edən əsas kateqoriyalardan biri də C&C (*ing. Command & Control, Komanda və Nəzarət*) serverləridir. Botmasterlər botlarla əlaqə saxlamaq üçün belə xüsusi serverlərdən istifadə edirlər [8]. C&C server kimi çox vaxt yerləşdiyi coğrafi ərazi məlum olmayan gizli serverlərdən istifadə olunur. Botmaster botneti idarə etmək üçün C&C server qurur və yoluxmuş kompüter hər hansı bir kanalla (məsələn, *IRC* (*ing. Internet Relay Chat*)) bu serverə bağlanır və ondan əmr gözləyir. Bir botnetdə birdən çox C&C server ola bilər ki, bu da onun aşkarlanmasını və məhv edilməsini çətinləşdirir. Botnetləri arxitekturasına görə bir neçə üsulla təsnif etmək olar. [9]-da botnetlər– mərkəzləşmiş, P2P (*ing. peer–to–peer*) və hibrid (ağacvari) kimi üç arxitekturada təsnif edilmişdir:

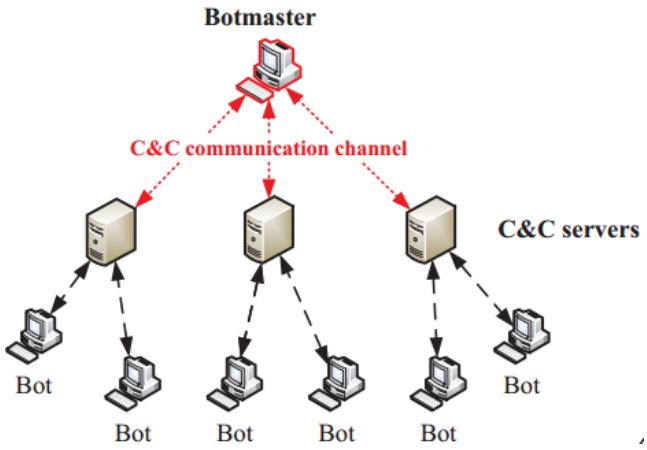
1) Mərkəzləşmiş C&C modeli (ing. Centralized C&C Model/).

Mərkəzləşmiş C&C modeli botnetlərdə istifadə olunan əsas modellərdən biridir. Ən çox tanınan botnetlərdən AgoBot, SDBot, Rbot və s. mərkəzləşmiş modelə aiddir. Belə modeldə botmaster botlarla əlaqə saxlamaq üçün bir yüksəksürətli kanal seçir. Adətən, belə modeldə C&C server IRC, HTTP kimi şəbəkə protokollarını istifadə edərək kompüteri "əməkdaşlığa" razı salır. Yeni kompüter botla yoluxduqda, o, C&C serverlə əlaqə yaradaraq botnetə qoşulur. Müvafiq C&C serverə bir dəfə qoşulduqdan sonra botmasterin əmrlərini gözləyir.

Mərkəzləşmiş C&C modelin istifadə edilməsinin aşağıdakı üstün cəhətləri var:

- daha asan əldə olunan proqramların (məsələn, IRC-skriptlər və IRC-botlar) istifadə olunması səbəbindən mərkəzləşmiş C&C modelində yoluxdurma və "özəlləşdirmə" daha sadədir. Belə modeli istifadə edərək botmaster eyni vaxtda minlərlə botu idarə edə bilər. Qazanc məqsədli botnetlər yaradılarkən daha çox botu idarə etməyə imkan verən və maksimum qazanc gətirən mərkəzləşmiş C&C modeli seçilir;
- mərkəzləşmiş modeldə mesajların gecikmə vaxtı çox kiçikdir. Bu da botmasterə botları rahat idarə etməyə və hücumlar təşkil etməyə imkan verir.

Lakin mərkəzləşmiş C&C modelinin zəif cəhətləri də vardır, belə ki, bütün mübadilələr mərkəzləşmiş server üzərindən aparıldığından, C&C server zəif halqa təşkil edir. Əgər C&C server aşkarlanarsa, bütün botnet çökmüş olur (şəkil 2).



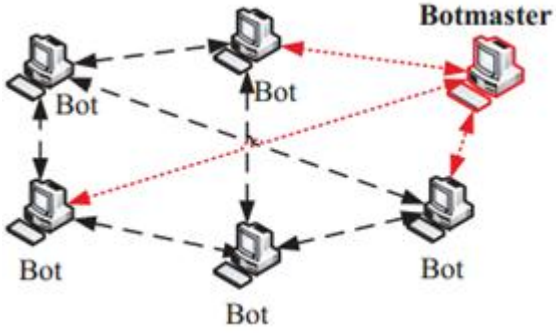
Şəkil 2. Mərkəzləşmiş C&C modeli

2) P2P-əsaslı C&C modeli (ing. P2P-Based C&C Model).

Şəbəkədə aşkarlanmalara daha davamlı hesab olunan botnet modellərindən biri də P2P-əsaslı (nöqtə-nöqtə birləşmiş, mərkəzi olmayan) C&C modelidir. P2P-əsaslı botnetlərin saylarının olduqca az olmasına baxmayaraq, mərkəzləşmiş modellə müqayisədə aşkarlanması və dağıdılması

daha çətindir. Mərkəzi olmayan botnetlərdə botlar idarəetmə mərkəzinə deyil, zombi-şəbəkənin bir neçə yoluxmuş maşınına qoşulur. Əmrlər botdan bota göndərilir, hər botda bir neçə "qonşunun" ünvanı olan siyahı olur və onların hər hansı birindən əmr alınan zaman o, əmri digər qonşularına ötürür, bununla da əmri yayır. Bu halda, botneti idarə etmək üçün botmasterin botnetə daxil olan ən azı bir kompüterə birbaşa çıxışı olmalıdır [10, 11].

Bu modellə qurulmuş botnetlərin getdikcə artmasına və daha çətin aşkarlanmasına baxmayaraq, mənfi cəhətləri də vardır. Birincisi, P2P sistemlər çox kiçik saylı (10–50) istifadəçi qrupları arasında əlaqəyə imkan verir. Bu miqyas mərkəzləşmiş modellə müqayisədə olduqca kiçikdir. İkincisi, P2P sistemlər mesajların vaxtında çatmasına və yayılmanın gecikməməsinə zamanət verə bilmir. Aktiv olmayan bir və ya bir neçə bot şəbəkədə yayılmanı kifayət qədər zəiflədə bilər. Ona görə də belə botnetləri idarə etmək çətindir. Bu iki səbəb P2P modelin daha geniş qəbulunu və istifadəsini məhdudlaşdırır (şəkil 3).



Şəkil 3. P2P-əsaslı C&C modeli

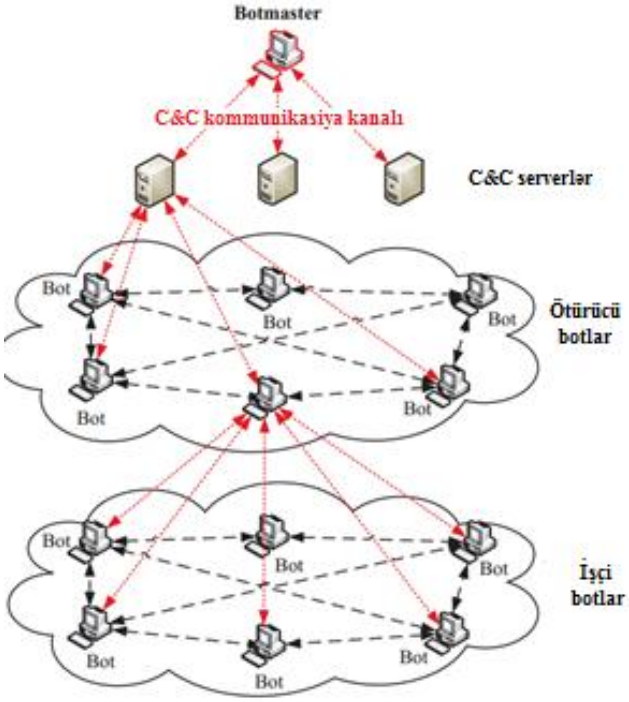
3) Hibrid C&C modeli (ing. Hybrid C&C Model).

Müasir botnetlər tərəfindən istifadə olunan C&C əlaqə formalarından biri də hibrid əlaqə formasıdır. Bu zaman kiçik gecikmələrə zəmanət vermək üçün mərkəzləşmiş və aşkarlanmaya qarşı dayanıqlıq üçün mərkəzi olmayan arxitektura birlikdə istifadə edilir. Belə arxitekturada botlar iki sinfə: *ötürücü* (*ing. proxy*) və *işçi* (*ing.working*) botlara bölünür. Ötürücü botlar daim botmaster və digər botlar arasında qarşılıqlı əlaqəni və əmrlərin yayılmasını həyata keçirir, işçi botlar isə yalnız ötürücü botlara bağlanır və botmasterdən gələcək əmrləri gözləyirlər (şəkil 4).

Botnetlər üçün xarakteristik kateqoriyalardan biri də C&C serverlərin işləmə mexanizmidir. Bu mexanizmlər yeni botlar tapmaq və onları botmasterdən asılı salmaq üçün vacibdir. Ən çox istifadə olunan mexanizmlər aşağıdakılardır [12,13]:

Sabit IP ünvanlar (*ing. Hard-coded IP address*). Bu üsulda bot ilk yoluxduğu anda sabit IP ünvanlı C&C serverlə əlaqə saxlayır. Bu üsulun mənfi cəhəti odur ki, sabit IP ünvan istifadə edən C&C serverləri asanlıqla aşkarlamaq və əlaqəni bloklamaq olar. Əgər bu zaman serverlə botlar arasında əlaqə kəsilirsə, botnet tamamilə məhv edilmiş olur. Ona görə də bu üsul müasir botnetlərdə, demək olar ki, istifadə olunmur.

Dinamik DNS (ing. DNS flux). Botnetlər DGA (*ing. Domain Generation Algorithm – Domen Yaratma Alqoritmi*) istifadə edərək kriptoqrafik üsullarla yaradılmış domen adları istifadə edirlər. Bu texnologiya statik sistemlər üçün bütün mümkün C&C ünvanları tapmağı olduqca çətinləşdirir. Əgər C&C server sahibi tərəfindən bağlanarsa, idarəetmə asanlıqla yeni serverə ötürülür. Köhnə serverlə əlaqəni itirən bot DNS sorğu göndərir və yeni C&C serverə qoşulur. Dinamik DNS adlar istifadə etməklə botmaster C&C server funksiyasını itirdikdə, onu bərpa edə bilir. Çox vaxt aşkarlamanı çətinləşdirmək üçün C&C serverlər tez-tez bilərəkdən dəyişdirilir.



Şəkil 4. Hibrid C&C modeli

Dinamik IP (*ing. IP flux*). Bu texnologiya FFSN (*ing. Fast Flux Service Networks – xidmət şəbəkələrinin sürətli dəyişməsi)* kimi də tanınır. FFSN şəbəkədə zərərli fəaliyyət göstərən botnet serverlərini gizlətmək üçün istifadə olunan bir DNS texnologiyasıdır. Bu texnologiyanın əsasını bir domen adı üçün birdən çox IP ünvanın saxlanması və bu ünvanların DNS keşinin daim dəyişdirilməsi təşkil edir. İki cür fast flux texnologiyası məlumdur: tək və ikiqat.

Bot kompüterə botnet sahibinin əmrlərini ötürmək üçün bot və əmr göndərən kompüter arasında şəbəkə bağlantısı yaratmaq lazımdır. Bütün şəbəkə qarşılıqlı əlaqəsi şəbəkə daxilində kompüterlərin kommunikasiya qaydalarını müəyyən edən şəbəkə protokollarına əsaslanır. Buna görə də, botnetləri istifadə olunan kommunikasiya protokolu əsasında təsnif etmək olar. İstifadə edilən şəbəkə protokollarının növünə görə botnetlər IRC, IM (*ing. Instant Messaging*), veb və digər (TCP, ICMP, UDP və s.) yönümlü qruplara bölünürlər.

Botnetlərin aşkarlanması üsullarının təsnifatı

2000-ci illərin əvvəllərindən başlayaraq, botnetlərin aşkarlanması üçün müxtəlif texniki prinsiplərə əsaslanan çox sayda yanaşmalar təklif olunmuşdur. Aşkarlama yanaşmaları iki əsas sinifdə klassifikasiya edilir: host-əsaslı (*ing. host-based*) və şəbəkə-əsaslı (*ing. network-based*). Host-əsaslı üsullar yoluxmuş maşında zərərli bot proqramının davranışlarını araşdırır. Bunun üçün tətbiq və sistem loqları, aktiv proseslər, açar-loqlar, resursların istifadəsi və s. kimi istifadəçi səviyyəsində davranışlar öyrənilir.

Şəbəkə-əsaslı aşkarlamada isə botnetlərin aşkarlanması üçün adətən marşrutlayıcı və ya şəbəkələrarası ekrandakı şəbəkə axını analiz edilir. Bu sinif aşkarlama üsulları bot fəaliyyəti dövrünün hər üç mərhələsində botlar tərəfindən yaradılan şəbəkə axınının tanınması ilə aşkarlamaya imkan verir. Belə aşkarlama üsulları çox vaxt müdaxilələrin aşkarlanması sistemləri (*ing. Intrusion Detection Systems, IDS*) və ya müdaxilələrin qarşısının alınması sistemləri (*ing. Intrusion Prevention Systems, IPS*) adlanır [14, 15].

Bundan əlavə, hər iki yanaşmanın birlikdə tətbiq edilməsi nəticəsində hibrid aşkarlama üsulları [16, 17]-da işlənmişdir. Bu sinif üsullar hər iki səviyyədə – həm istifadəçi səviyyəsində davranışları, həm də şəbəkə səviyyəsində şəbəkə axınını birlikdə analiz edir.

Qeyd etmək lazımdır ki, host-əsaslı üsullar istifadəçi səviyyəsində istifadə olunan dayanıqlılığı artırma üsullarına qarşı olduqca zəifdir. Botmaster bot proqramların yoluxmuş maşında aşkarlana bilməməsi üçün müxtəlif üsullar tətbiq edir və host-əsaslı üsullar yalnız yoluxmuş bir botu və onun C&C əlaqələrini aşkarlamağa imkan verir. Şəbəkə-əsaslı üsullar isə yoluxmuş maşınların şəbəkə aktivliklərini (spam göndərilməsi, DDoS-hücum və s.), həmçinin C&C serverlə istənilən əlaqə cəhdlərini araşdırır. Şəbəkə-əsaslı üsulların əsas üstünlüyü çox sayda yoluxmuş maşını müşahidə etməyə və aşkarlamağa imkan verməsidir.

Şəbəkə-əsaslı aşkarlama

Şəbəkə-əsaslı aşkarlama [18] üsulları yoluxmuş maşınları aşkarlamaq üçün şəbəkə axınının analizinə əsaslanır. Şəbəkə trafikini paket və şəbəkə axını səviyyəsində analiz etmək olar. Şəbəkə axını adətən beş əsas əlamət: göndərən (*ing. source*) və alan (*ing. destination*) IP-ünvanlar, göndərən və alan portlar və protokol göstəricisinə görə müəyyən edilir. Lakin real aşkarlama üsullarında daha çox axın əlaməti analiz edilə bilər. Şəbəkə-əsaslı üsullar özləri də tətbiq edilmə nöqtəsi, əməliyyatların gizliliyi, əsas işləmə prinsiplərinə görə bir neçə sinfə bölünürlər.

Şəbəkə-əsaslı aşkarlama üsullarının müxtəlifliyi ilk növbədə üsulun şəbəkə trafikinin hansı hissəsində tətbiq olunmasından asılıdır. Aydındır ki, daha çox botu aşkarlamağa yönəlmiş şəbəkə-əsaslı üsullar böyük həcmdə verilənlərlə işləməyə imkan verməlidirlər [19].

Gizlilik funksiyasının ödənməsinə görə aşkarlama üsulları *aktiv* və *passiv* kimi iki sinfə ayrılırlar. Passiv aşkarlama yanaşmaları botnet əməliyyatlarına müdaxilə etmir, onları yalnız müşahidə edir ki, bu da aşkarlama əməliyyatlarını gizli edir və botmasterlər tərəfindən hiss edilmir. Aktiv aşkarlama üsulları isə botnetlərin zərərli fəaliyyətlərinə və ya C&C serverlə istənilən əlaqə cəhdlərinə aktiv şəkildə müdaxilə edə bilirlər. Adətən, belə üsullar evristik C&C əlaqələri hədəf alır və yanaşmanın elastikliyi və ümumiliyi bahasına yüksək aşkarlama dəqiqliyini təmin edirlər. Bu baxımdan passiv yanaşmaların əsas üstünlüyü yalnız müşahidə edilən zərərli trafik siqnaturalarına (obrazlarına) görə böyük ölçüdə botnet tiplərini aşkarlaya bilməsidir. Mövcud aşkarlama üsullarının əksəriyyəti passivdir, çox az sayda aktiv üsullar vardır.

Aşkarlama üsulları əsas funksional işləmə prinsipinə görə iki sinfə – *siqnatura-əsaslı* və *anomaliya-əsaslı* siniflərə ayrılır. Siqnatura-əsaslı üsullar "siqnatura" adlanan xarakteristik trafik obrazlarının tanınmasına əsaslanır. Bu sinif aşkarlama üsulları botnet fəaliyyət dövrünün istənilən mərhələsində tətbiq edilə bilir və məlum botnetlərin yüksək dəqiqliklə aşkarlanmasını təmin edirlər. Lakin üsulun əsas zəif cəhəti yalnız məlum təhlükələri aşkarlaya bilməsidir və bu yanaşma siqnaturaların vaxtaşırı yenilənməsini tələb edir.

Anomaliya-əsaslı aşkarlama üsulları isə şəbəkə trafikində baş verən anomaliyalara görə zərərli trafikin aşkarlanmasına əsaslanırlar. Belə üsullar şəbəkə trafikininin səviyyəsinin dəyişməsi, gecikmələr və s. kimi asan aşkarlana bilən şəbəkə hadisələrinə əsaslanır. Bu sinif yanaşmalar paket və axın səviyyəsində işləyə bilir. Anomaliya-əsaslı yanaşmada statistik analiz, MT, qrafların analizi və s. üsulları tətbiq edilir. Siqnatura-əsaslı üsullardan fərqli olaraq, anomaliya-əsaslı aşkarlama yanaşmaları yeni təhlükələri də aşkarlaya bilir və botnetlərin gizlilik tədbirlərinə qarşı dözümlüdürlər. Müasir botnetlərin istifadə etdikləri trafik normal trafikə olduqca oxşardır, buna görə də şəbəkədəki hansı hadisələrin anomal qəbul olunması əhəmiyyətli məsələlərdən biridir. Həmçinin anomal aşkarlama zamanı çox böyük ölçüdə verilənlərin analiz edilməsi lazım gəldiyindən, bu sahədə ən çox istifadə olunan yanaşmalar MT üsullarının tətbiqi ilə analizdir. Çünki MT üsulları bot əlaqəli trafik obrazlarının köməyi ilə avtomatik tanınma təklif edir və zərərli trafik əlamətləri haqqında əvvəlcədən məlumat olmadığı halda zərərli trafik obrazlarının tanınmasına imkan verir.

MT üsullarının tətbiqi ilə çox sayda aşkarlama üsulları təklif olunmuşdur. Onlardan ən effektiv nəticələr əldə etməyə imkan verən üsullara BotMiner [20], BotGAD [21], BotSniffer [22], BotHunter [23], EFFORT [24] və s. misal göstərmək olar.

MT əsasında botnetlərin aşkarlanması

MT [25, 26] süni intellektin bir qoludur və əsas məqsədi sonlu sayda əvvəlki təcrübələrə əsasən biliyin ümumiləşdirilməsi və əvvəlcədən bilinməyən hadisələr üçün yararlı qanunauyğunluqların tapılmasıdır. MT üsullarının əsas üstünlüyü böyük həcmdə verilənlərin içərisindən lazım olan biliyi tapa bilməsidir. MT üsulları bir çox sahədə – statistika, süni intellekt, informasiya nəzəriyyəsi, koqnitiv elmlər, idarəetmə nəzəriyyəsi və s. kimi sahələrdə tətbiq olunur. MT alqoritmlərinin tətbiq olunduğu sahələrdən biri də botlarla əlaqəli şəbəkə trafikinin aşkarlanmasıdır.

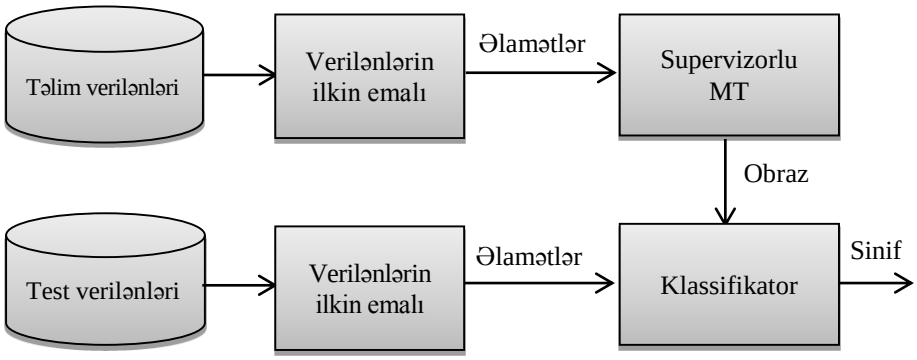
MT alqoritmləri iki əsas sinfə bölünürlər:

- supervizorlu öyrənmə (*ing. supervised learning*);
- supervizorsuz öyrənmə (*ing.unsupervised learning*);

Supervizorlu öyrənmə ən çox tətbiq edilən MT üsullarındandır ki, burada alqoritmlər giriş nümunələri və onlara uyğun çıxışlara görə öyrədilir və daha sonra hər hansı yeni girişlər üçün çıxışın proqnozlaşdırılmasında istifadə olunurlar. Supervizorlu öyrənmə giriş verilənlərinin hər hansı müəyyən olunmuş sinfə aid edilməsində və çıxışda proqnozlaşdırılmış qiymətin verilməsində istifadə olunur.

Supervizorsuz öyrənmə problemlərində hədəf giriş verilənləri içərisində oxşar nümunələri tapmaq – *klasterizasiya*, giriş fəzasında verilənlərin paylanmasını müəyyənləşdirmək – *sıxlığın qiymətləndirilməsi* və ya çoxölçülü fəzadakı verilənləri təsəvvür etmək məqsədilə 2- və ya 3-ölçülü fəzaya gətirmək məsələsi ola bilər.

Anomaliya-əsaslı botnet aşkarlamada əksər hallarda klasifikasiya və ya klasterizasiya kimi supervizorlu və ya supervizorsuz MT alqoritmləri istifadə olunur. Şəbəkə trafiki hər iki istiqamətdə (giriş və çıxış) analiz edilir və paket səviyyəsində əlamətlər çıxarılır. Çıxarılmış trafik əlamətləri xüsusi trafik axınını və ya şəbəkədə xüsusi server və hostları təsvir edir. Supervizorlu MT alqoritmlərinin tətbiqi ilə botnet aşkarlama üsullarının ümumi sxemi aşağıdakı kimidir (şəkil 5).

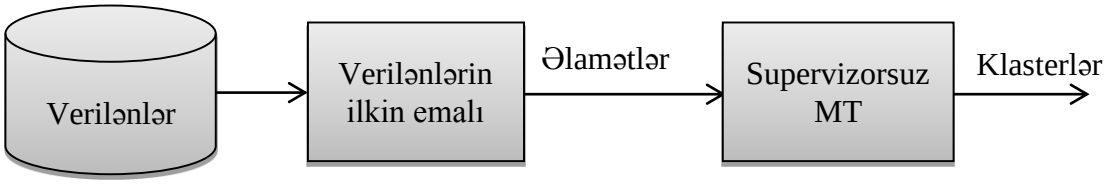


Şəkil 5. Supervizorlu aşkarlama sxemi

Supervizorlu MT alqoritmləri əvvəlcə təlim verilənləri ilə öyrədilir və uyğun giriş-çıxışlara görə funksiya yaradılır. Bu funksiya daha sonra model kimi test verilənlərindəki girişləri klassifikasiya etmək üçün istifadə olunur. Supervizorlu MT üsullarından istifadə edilməsi üçün hər iki verilənlər çoxluğu – test və təlim verilənləri ilkin emaldan keçməlidir. Verilənlərin ilkin emalı bir neçə prosesin birlikdə tətbiqini nəzərdə tutur və əlamətlərin seçilməsini təmin edir. MT alqoritminin praktik olaraq tətbiqi zamanı düzgün işləməsi üçün doğru əlamətlərin seçilməsi çətin problemlərdən biridir. Çünki doğru əlamətlərin seçilməməsi və ya səhv seçilməsi aşkarlamanın keyfiyyətinə birbaşa təsir edir. Əlamətlər botnetlərin evristik xassələrinə, C&C əlaqə kanalının növünə, istifadə olunmuş protokola və s. əsaslanmaqla seçilə bilər. Botnet aşkarlama üçün ən çox istifadə olunan supervizorlu MT üsulları SVM (*ing. Support Vector Machines – dəstək vektorları*

metodu), süni neyron şəbəkələri, qərar ağacları, Bayes şəbəkələri və başqalarıdır.

Supervizorlu öyrənmədən fərqli olaraq, supervizorsuz öyrənmə üsulları bot-əlaqəli verilənlərin klasterləşdirilməsi üçün istifadə olunurlar. Supervizorsuz MT alqoritmlərinin əsas xarakteristik əlaməti əvvəlcədən təlim keçilməsini tələb etməməsidir. Supervizorsuz MT alqoritmlərinin tətbiqi ilə botnet aşkarlamanın ümumi sxemi aşağıdakı kimidir (şəkil 6):



Şəkil 6. Supervizorsuz aşkarlama sxemi

Bu üsullarda əlamətlərin çıxarılması və seçilməsi üçün ilkin emal və supervizorsuz MT alqoritmləri istifadə edilərək verilənlərin klasterləşdirilməsi aparılır. Bu tip aşkarlama üsullarının əsas problemi müvafiq əlamətlərin seçilməsi və klasterlərin adlandırılmasıdır. Botnet aşkarlama üçün istifadə olunan ən məşhur supervizorsuz MT alqoritmləri K-means, X-means və iyerarxik klasterizasiyadır.

Botnetlərin aşkarlanması üçün hər iki ssenari üzrə MT üsullarının tətbiqi zamanı verilənlərin ilkin emalı və botnetləri uğurla aşkarlaya bilən əlamətlərin çıxarılması əhəmiyyətli prosesdir. Bundan əlavə müasir aşkarlama üsullarında daha keyfiyyətli aşkarlama üçün çox vaxt MT alqoritmləri birlikdə kombinasiya şəklində tətbiq olunurlar.

Aşkarlama üsullarının əsas prinsipləri

MT əsasında botnetlərin aşkarlanması müasir yanaşma hesab olunur və aşağıdakı kimi bir sıra əsas əlamətləri vardır:

1) Ümumilik (*ing. Generality*);
2) Gizlilik (*ing. Stealthiness*);
3) Vaxtında aşkarlama (*ing.Timely detection*);
4) Yüksək aşkarlama məhsuldarlığı (*ing. High detection performances*);
5) Yayınma üsullarına qarşı dayanıqlıq (*ing. Robustness on evasion techniques*).

Üsulun ümumiliyi dedikdə, eyni bir üsulun yayılma mexanizmlərindən, hücum hədəflərindən, istifadə etdikləri C&C əlaqə kanalından asılı olmadan müxtəlif tip botnetlərin aşkarlanmasına tətbiq oluna bilməsinin mümkünlüyü nəzərdə tutulur. Aşkarlama üsulu ilk olaraq botnet fəaliyyət dövrünün yoluxma, əlaqə və ya hücum mərhələlərindən birində tətbiq oluna bilər. Aydındır ki, botnetin ilkin və ya təkrar yoluxma mərhələsində aşkarlanması onların sonrakı fəaliyyətlərinin qarşısının alınması baxımından daha effektiv nəticələr verə bilər. Lakin bu kifayət qədər çətindir, çünki bilavasitə aşkarlamaq üçün informasiya azdır və yoluxma mərhələsində istifadə olunan üsulların müxtəlifliyi bot zərərvericiləri "yaxşı" gizlədir.

Əlaqə mərhələsində tətbiq olunan aşkarlama yanaşmaları müxtəlif əlaqə protokollarına (IRC, HTTP, P2P və s.) və botnet şəbəkə topologiyalarına yönəlir. İlk belə aşkarlama üsulları əsasən IRC trafiki hədəfləyirdi. Lakin müasir botnetlər daha çox P2P və HTTP protokolları istifadə etdiyinə görə aşkarlama üsulları da daha çox bu protokollara yönəlmişdir.

Hücum mərhələsində fəaliyyət göstərən üsullarda isə konkret hücum cəhdləri (spam, DDoS və s.) hədəflənir. Belə aşkarlama üsullarında adətən qrup şəklində yoluxmuş kompüterlərin aktivlik sıxlıqları analiz edilir və normal trafik sıxlığından əhəmiyyətli kənaraçıxmalar bot xəbərdarlığı kimi qəbul edilə bilir.

Bundan əlavə, botnet aşkarlamanın ümumiliyi yanaşmanın bot-əlaqəli evristik fərziyyələri və onların real botnetlərdə özünü necə əks etdirməsindən asılıdır. Konkret tip botnetləri və ya konkret fəaliyyət dövrünü hədəfləyən yanaşmalar bir çox hallarda bütün tip botnetləri hədəfləyən

universal üsullardan daha effektiv nəticələr verir. Nəzərə almaq lazımdır ki, botlar bədniyyətliyə uzunmüddətli istifadə üçün lazımdır və onlar əlaqə protokolunu və ya C&C əlaqə kanalını lazım gəlmədikcə dəyişmirlər. Lakin buna baxmayaraq, konkret üsullar botnetlərin təbiətindəki istənilən dəyişikliyə qarşı zəif uyğunlaşa bilirlər.

Gizlilik – aşkarlama yanaşmasının hücum edənlər tərəfindən hiss edilə bilməməsidir, belə ki, bütün passiv üsullar öz fəaliyyətləri müddətində gizlidir. Təklif olunmuş aşkarlama yanaşmalarının əksəriyyəti passivdir və öz fəaliyyətlərində gizlilik şərtini ödəyirlər.

Vaxtında aşkarlama – çox vaxt üsulun onlayn rejimdə işləməsini tələb edir ki, bu da üsulun real vaxtda böyük həcmli verilənləri analiz etmə imkanına malik olmasına gətirib çıxarır. Lakin müasir üsulların bir çoxu haqqında vaxtında aşkarlama şərtini ödədiyini söyləmək çətindir.

Aşkarlamanın keyfiyyəti

Aşkarlama üsullarının keyfiyyəti əldə etdikləri real nəticələr və həssas olduqları yayınma texnologiyalarının qiyməti ilə ölçülür. Üsulun qiymətləndirilməsi adətən xüsusi seçilmiş verilənlər bazası vasitəsilə aparılır. Test verilənləri zərərli və zərərsiz trafik verilənlərindən ibarət ola bilər. Düzgün seçilmiş verilənlər çoxluğu aşkarlamanın keyfiyyətini qiymətləndirmək üçün əsas şərtlərdən biridir. Zərərli trafik botnetlər tərəfindən yaradılan trafik kimi təqdim olunur, zərərsiz trafik isə çox vaxt "arxa fon" adlandırılır və zərərsiz hostlar tərəfindən yaradılan "təmiz" trafikdən ibarət olur. Bot-əlaqəli trafik aşağıdakı qaydalarla əldə edilə bilər [27]:

1) Bot-əlaqəli trafik xüsusi qurulmuş honeypotlar tərəfindən toplana bilər;
2) Bot-əlaqəli trafik tam nəzarət edilən təşkilat şəbəkələrindən toplana bilər;
3) Bot-əlaqəli trafik qismən nəzarət edilən təşkilat şəbəkələrindən toplana bilər.

Zərərsiz trafikin seçilməsi özü də kifayət qədər problemli məsələdir və müxtəlif yollarla, məsələn, statik trafik generatoru istifadə etməklə, lokal şəbəkələrdə snifferlər vasitəsilə, hətta ISP (*ing. Internet Service Provider*) şəbəkələrindən də toplana bilər.

Aşkarlama yanaşmalarının keyfiyyət metrikaları müxtəlifdir, ən çox istifadə olunan metrikalar aşağıdakılardır:

1) Doğru müsbətlərin faizi (*ing. True positives rate* (*TPR*)): $TPR = \frac{TP}{TP+FN}$.
2) Doğru mənfilərin faizi (*ing. True negative rate (TNR*)): $TNR = \frac{TN}{TN+FP}$.
3) Yanlış müsbətlərin faizi (*ing. False positive rate (FPR*)): $FPR = \frac{FP}{FP+TN}$.
4) Yanlış mənfilərin faizi (*ing. False negative rate (FNR*)): $FNR = \frac{FN}{FN+TP}$.
5) Dəqiqlik (*ing. Accuracy*): $accuracy = \frac{TP+TN}{TP+FP+TN+FN}$.
6) Səhv (*ing. Error*): $error = \frac{FP+FN}{TP+FP+TN+FN}$.
7) Həssaslıq (*ing. Precision*): $precision = \frac{TP}{TP+FP}$.

Burada *TP* – doğru klassifikasiya edilən müsbət nümunələrin sayı, *TN* – doğru klassifikasiya edilən mənfi nümunələrin sayı, *FP* – yanlış klassifikasiya edilən müsbət nümunələrin sayı, *FN* – yanlış klassifikasiya edilən və mənfi olan nümunələrin sayıdır. Lakin yanaşmanın keyfiyyətinin ölçülməsi üçün yuxarıda qeyd olunan metrikaların hamısı həmişə istifadə olunmur. Ən çox istifadə olunan metrikalar *TPR* və *FPR* faizləridir. *TPR* faizinin kifayət qədər böyük, *FPR* faizinin isə kifayət qədər kiçik olması aşkarlama yanaşmasının keyfiyyətini müəyyənləşdirir.

Nəticə

Botnetlər ölkələrin kritik informasiya resurslarına genişmiqyaslı kiber-hücumların həyata keçirilməsində əsas vasitələrdən biridir. İstər DDoS hücumların sayı, istərsə də botnetlərin səbəb olduğu digər problemlər onların nə qədər təhlükəli olduğunu sübut edir. Botnetlərin qarşısının

alınması, zamanında aşkarlanması və onlara qarşı ehtiyat tədbirlərinin həyata keçirilməsi vacibdir. Bu işdə aparılmış analizlər göstərir ki, botnetlərin aşkarlanmasına yanaşmalar MT və verilənlərin intellektual analizi metodlarına əsaslanır. Gələcək tədqiqatların bu istiqamətdə aparılması planlaşdırılır.

Ədəbiyyat

1. Liu J., Xiao Y., Ghaboosi K., Deng H., Zhang J. Botnet: classification, attacks, detection, tracing, and preventive measures // EURASIP Journal on Wireless Communications and Networking, 2009, pp.1–12.
2. Li C., Jiang W., Zou X. Botnet: survey and case study / Proc. of the 4th International Conference on Innovative Computing, Information and Control, 2009, pp.1184–1187.
3. McKewan A. Botnets – zombies get smarter // Network Security, 2006, vol.2006, no.6, pp.18–20.
4. Schiller C.A., Binkley J., Evron G., Willems C., Bradley T., Harley D., Cross M. Botnets: the killer web app. Syngress, 2007, 480 p.
5. Rodrigues N., Sousa R., Ferreira P.S., Nogueira A.M. Characterization and modeling of top spam botnets // Network Protocols and Algorithms, 2012, vol.4, no.4, pp.1–26.
6. Silva S.S., Silva R.M., Pinto R.C., Salles R.M. Botnets: A survey // Computer Networks, 2013, vol.57, no.2, pp.378–403.
7. Feily M., Shahrestani A., Ramadass S. A survey of botnet and botnet detection / Proc. of the 3rd International Conference on Emerging Security Information, Systems and Technologies, 2009, pp.268–273.
8. Zeidanloo H., Manaf A. Botnet command and control mechanisms / Proc. of the 2nd International Conference on Computer and Electrical Engineering (ICCEE'09), 2009, vol.1, pp.564–5683.
9. TrendMicro. Taxonomy of botnet threats. Technical Report, 2006. http://www.cs.ucsb.edu/kemm/courses/cs595G/TM06.pdf
10. Rodríguez-Gómez R.A., Maciá-Fernández G., García-Teodoro P., Steiner M., Balzarotti D. Resource monitoring for the detection of parasite P2P botnets // Computer Networks, 2014, vol.70, pp.302–311.
11. Singh K., Guntuku S. C., Thakur A., Hota C. Big Data Analytics framework for peer-to-peer botnet detection using Random Forests // Information Sciences, 2014, vol.278, pp.488–497.
12. Sharifnya R., Abadi M. DFBotKiller: Domain-flux botnet detection based on the history of group activities and failures in DNS traffic // Digital Investigation, 2015, vol.12, pp.15–26.
13. OpenDNS Security Whitepaper. The role of DNS in botnet command & control. http://info.opendns.com/rs/opendns/images/OpenDNS_SecurityWhitepaper DNSRoleInBotnets.pdf
14. Jabez J., Muthukumar B. Intrusion Detection System (IDS): Anomaly detection using outlier detection approach // Procedia Computer Science, 2015, vol.48, pp.338–346.
15. Kacha C., Shevade K.A. Comparison of different intrusion detection and prevention systems // International Journal of Emerging Technology and Advanced Engineering, 2012, vol.2, no.12, pp.243–245.
16. Zeng Y., Hu X., Shin K. Detection of botnets using combined host and network level information / IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2010, pp.291–300.
17. Zeng Y. On detection of current and next-generation botnets. Ph.D. thesis. The University of Michigan, January 2012.
18. Zhao D., Traore I., Sayed B., Lu W., Saad S., Ghorbani A., Garant D. Botnet detection based on traffic behavior analysis and flow intervals // Computers &Security, 2013, vol.39, part A, pp.2–16.

19. Stevanovic M., Pedersen J.M. Machine learning for identifying botnet network traffic, Aalborg Universitet, Technical Report, 2013, 29 p.
20. Gu G., Perdisci R., Zhang J., Lee W. Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection / Proc. of the 17th Conference on Security Symposium, 2008, pp.139–154.
21. Choi H., Lee H. Identifying botnets by capturing group activities in DNS traffic // Journal of Computer Networks, 2011, vol.56, pp.20–33.
22. Gu G., Zhang J., Lee W. BotSniffer: detecting botnet command and control channels in network traffic / Proc. of the 15th Network and Distributed System Security Symposium (NDSS), 2008, pp.1–18.
23. Gu G., Porras P., Yegneswaran V., Fong M., Lee W. BotHunter: Detecting malware infection through IDS-driven dialog correlation / Usenix Security, 2007, vol.7, pp.1–16.
24. Shin S., Xu Z., Gu G. EFFORT: Efficient and effective bot malware detection / Proc. of the 31th Annual IEEE Conference on Computer Communications (INFOCOM'12) Mini-Conference, 2012, pp.71–80.
25. Masud M., Khan L., Thuraisingham B. Data Mining Tools for Malware Detection. Taylor & Francis Group, 2011.
26. Dua S., Du X. Data Mining and Machine Learning in Cybersecurity, CRC Press, 2011, 248 p.
27. Aviv A. J., Haeberlen A. Challenges in experimenting with botnet detection systems / Proc. of the 4th Conference on Cyber Security Experimentation and Test (CSET'11), 2011, pp.6.

УДК 004.9:351

Имамвердиев Ядигар Н.[1], Гараева Гульнара Б.[1,2]
[1]Институт Информационных Технологий НАНА, Баку, Азербайджан
[2]Шекинский филиал АГПУ, Шеки, Азербайджан
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru

Ботнеты и методы их обнаружения

Ботнеты занимают важное место в инфраструктура кибератак, иногда в этой сети участвуют миллионы компьютеров. Ботнет представляет собой сеть из зараженных компьютеров и серверов C&C, которые управляются ботмастерами. Ботнеты постоянно развиваются, структуры, используемые протоколы, методы заражения, цель атаки постоянно меняются. В статье были исследованы архитектура, классификация по разным критериям и методы обнаружения ботнетов.

Ключевые слова: *ботнет, C&C серверы, honeypot, DDoS атаки, методы обнаружения ботнетов.*

Yadigar N. Imamverdiyev[1], Gulnara B. Garayeva[1,2]
[1]Institute of Information Technology of ANAS, Baku, Azerbaijan
[2]Sheki branch of ASPU, Sheki, Azerbaijan
[1]yadigar@lan.ab.az, [2]qarayevagulnare@mail.ru

Botnets and methods of their detection

Botnets have an important place in the infrastructure of cyber attacks, sometimes millions of computers are involved in these networks. A botnet is a network of infected computers and the C & C servers, which are managed by botmasters. Botnets are constantly evolving - their structure, used protocols, infection methods, purposes of attacks are constantly changing. The paper studies the architecture of botnets, classification of botnets according to various criteria and botnet detection methods.

Keywords: *botnet, C&C server, honeypot, DDoS attack, botnet detection method.*